Chapter 37 - Storage and Destruction Equipment

3701 Physical Protection and Storage of Materials

A. Employees or others having custody of classified or sensitive information or Federal Government property are responsible for its safeguarding and proper handling. The policy and procedures for the safe handling of such information are set forth in Chapters 23, Custody and Accountability, and 24, Storage, of the Security Manual detailing the physical storage and destruction requirements for such material.

B. Many types of storage equipment are used to store classified and sensitive information, weapons, controlled substances, valuable equipment, and negotiable documents or funds. Only equipment described in this manual or specifically approved by the Office of Security may be used to store such materials.

C. To minimize the possibility of compromise of classified information or attempts to break into and enter security storage equipment, such items as money, weapons, narcotics, and precious metals will not be stored in any security storage equipment in which classified information is stored.

D. The heads of operating units and departmental offices are responsible for ensuring that authorized equipment is utilized for the protection of classified and sensitive information and property, and that employees are made aware of such requirements.

3702 Security Containers

Security containers used to store classified information at the Secret level and above will be controlled through the Department's electronic database system, Security Information Management System (SIMS), where possible, or by other database systems. Each operating unit is responsible for entering information into this electronic system and for assisting the security contact in maintaining a record of controlled information.

A. Approved Containers. Federal specifications for security containers are developed by the Interagency Advisory Committee on Security Equipment (IACSE), which also approves equipment listed on GSA's Federal Supply Schedule. A security container approved by GSA for storing classified information will bear a label affixed to the exterior attesting to its storage capability. Approved containers are those rated Class 1, Class 5, or Class 6 on the GSA's Federal Supply

Schedule list. Older containers will normally have such an approval label affixed to the inside of the control drawer, however, the label may be missing from some containers as a result of age, damage, rehabilitation, or other modification.

B. Types of Security Containers.

1. **Class 1** containers, insulated for fire protection and available in 2- and 4-drawer models, are authorized for storage of classified material up to, and including, Top Secret. The protection provided is:

30 man-minutes against surreptitious entry;
20 man-hours against lock manipulation;
20 man-hours against radiological attack;
10 man-minutes against forced entry; and
1 man-hour against fire damage to contents.

2. **Class 5** containers are not insulated for fire protection and are available in 2-, 4-, and 5-drawer models. These containers are authorized for storage of classified material up to, and including, Top Secret. It is certified for:

30 man-minutes against surreptitious entry;
20 man-hours against lock manipulation;
20 man-hours against radiological attack; and
10 man-minutes against forced entry.

3. **Class 6** containers afford the same protection as the Class 5, however, there is no certified forced entry protection. These containers are designed with 2-, 4-, or 5-drawers and are authorized for storage of classified material up to, and including, Top Secret. It provides the following protection:

30 man-minutes against surreptitious entry;
20 man-hours against lock manipulation;
20 man-hours against radiological attack; and
No forced entry test requirement.

4. **Map and Plan Security Cabinets.** Security cabinets that are manufactured in both Class 5 and Class 6 models. The Map and Plan security cabinet can be equipped with individually locked compartments and is authorized for storage of classified material up to, and including, Top Secret.

5. **Money Safes.** Class 5 containers that come with or without a channel base. For information related to the storage of funds, see paragraph 3803, Protection of Funds, and Appendix P, Disbursing Office and Imprest Fund Checklist. Additional information can be obtained from the Department's Cash Management Handbook and the Treasury Department's Manual of Procedures and Instructions for Cashiers.

6. **Weapons Storage Containers.** Class 5 containers that come with a standard 7-drawer configuration.

7. **Vaults.** Storage container that is used for the storage of classified information, providing the vault meets the construction standards specified in DCID 1/21, Physical Security Standards for Sensitive Compartmented Information Facilities. Prior to constructing or utilizing such a facility, managers must consult with their servicing security officer for certification of the vault for storage of classified information.

C. Procuring Storage Containers. Prior to procuring new storage containers, managers should make an effort to retire, return, declassify, or destroy unneeded classified records, files, or materials to make storage space or containers available. Managers should also check with property management personnel to determine if surplus containers are available prior to purchase of new containers.

D. Conditionally Approved Containers.

1. For a number of years, a large number of filing cabinets with security lock-bars and padlocks have been conditionally approved for classified storage up to the Secret level. Lock-bar filing cabinets are easily compromised, however, and do not provide adequate protection for classified information. Therefore, these containers must be phased out of use by October 1, 2012. Until October 1, 2012, material up to the Secret level may be stored only if the equipment is already in use. These cabinets must be systematically phased out and be replaced with newer GSA-approved security containers.

2. Older containers manufactured by Remington-Rand and Shaw-Walker are approved only for the storage of information up to the Secret level. These models should be systematically phased out of service as resources permit.

SAFETY NOTE: GSA determined that several Remington-Rand and Shaw-Walker cabinets, which were rated as fire retardant or fire resistant, contain asbestos that can be released into the atmosphere through normal

use. Those models should be identified and given priority consideration for replacement. Managers should call their servicing security officer if they have any questions about the identity of these containers.

E. Non-approved Containers. A filing cabinet is a container designed as a file storage unit with no inherent security features. Currently, there are no filing cabinets on the market that are approved by the Department for the storage of classified information.

F. Accountability of Storage Equipment.

1. The security contact or servicing security officer must maintain a record on any vault, secure room, or container used to store classified information. The SF-700, Security Container Information, shall be used for this purpose.

2. To identify each vault or container, the security contact or servicing security officer will externally mark each container and vault door with a number or symbol. This will aid in the accountability process and will facilitate the maintaining of combinations by safe and room number.

3. The container should not have any external marking to indicate the type of contents or classification level of information stored within the container or vault.

4. Access to the combination of a vault or container used for storing classified information may be given only to those individuals who have the appropriate clearance and need-to-know.

G. Moving Security Containers. When security containers are moved from one location to another, even within the same building, the precautions listed below must be taken.

1. The security contact shall be notified of all container moves and coordinate the move with the responsible official. The security contact shall inform the servicing security officer of the move within 24 hours of the move.

2. Security containers must be securely locked, clearly and distinctly marked to show the new destination, and be accompanied by an appropriately cleared employee of the office or facility while in transit.

3. Containers of classified information must be stored within a locked or otherwise secured room. Under no circumstances should the container be left unattended.

4. The Classified Control Point (CCP) will update the SIMS database to reflect the new location of the security container.

H. Repairing Security Containers.

1. Persons who repair or drill security containers, vault doors, and locks must be cleared for access to the highest level of classified information stored within the container or must be escorted and continuously watched while working on the container.

2. Although repaired containers cannot be used to store Top Secret information, GSA-approved containers can be returned to their original state of security for storage up to the Secret level by meeting the following conditions.

a. All damaged or altered parts must be replaced.

b. When a container is drilled adjacent to or through the dial ring, the lock must be replaced with a computerized combination lock meeting Federal Specification FF-L-2740. The drilled hole must be repaired with a tapered casehardened steel rod (dowel, drill bit, bearing) with a diameter and length slightly larger than the hole. When the rod is driven into the hole, a shallow recess should remain at each end of the rod that is no less than one-eighth inch or 3.175 mm or more than three-sixteenths inch or 4.76 mm deep. This will permit a substantial weld on the inside and outside surfaces. The outside of the drawer head must then be puttied, sanded, and repainted in such a way that no visible evidence of the hole or its repair remains on the outer surface after replacement of the damaged parts.

c. Containers that have been drilled or repaired in a manner other than that described above cannot be restored to their original state of security integrity. The "Test Certification Label" and the "General Services Administration Approved Security Container" label, if any, must be removed. The container must not be used for storing classified information and a notice to this effect must be marked on the front of the container. Labels can be obtained from the Office of Security.

I. Disposing of Excess or Obsolete Containers. Prior to surplusing a storage container, the security contact or container custodian must remove all drawers and search inside to ensure that classified material is not inadvertently left in the container. The combination must be reset to the factory setting 50-25-50. A written statement must be placed on the container attesting to the fact that the container was checked and the combination reset.

3703 Destruction Equipment

To properly destroy classified or sensitive material, personnel should use equipment appropriate for the type of material being destroyed. See paragraph 2307, Destruction of Classified Material, for further guidance regarding the destruction of classified information.